UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information Associated with the Email Account **HKULLAH@GMAIL.COM** That is Stored at Premises Controlled by Google

Case No. 1:19-SW-445

UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1028A	Aggravated Identity Theft
18 U.S.C. § 287	Submission of False Claims

The application is based on these facts:

See attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

Russell L. Carlberg, SAUSA

Applicant's signature

Special Agent Lisa Warffeli, U.S. Dept. of State, OIG

Printed name and title

Sworn to before me and signed in my presence.

Date: 4/25/19

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

Judge's signature

City and state: Alexandria, Virginia

The Hon. Theresa Carroll Buchanan, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the following email account:

hkullah@gmail.com

which is stored at premises controlled by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google

For the account listed in Attachment A, to the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any e-mails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved since October 31, 2018, Google is required to disclose the following information to the government for the period of account inception to the present:

a. The contents of all electronic communications associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, files, all attachments to emails and other communications (including the native files), the source and destination addresses associated with each communication, all email header information, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All device information associated with the account;

e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, chat lists, calendar data, pictures, and files;

f. All records pertaining to communications between USAGM and any person regarding the account, including contacts with support services and records of actions taken.

g. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of wire fraud (18 U.S.C. § 1343), aggravated identity theft (18 U.S.C. § 1028A), and false claims (18 U.S.C. § 287), involving HAROON K. ULLAH and any other co-conspirators, including, for the email account listed on Attachment A, information pertaining to the following matters:

a. The email and information will contain evidence that ULLAH is involved in defrauding the United States through the submission of fraudulent vouchers and falsified supporting invoices and receipts, as described in the Affidavit in support of probable cause. The account will contain evidence of communications between ULLAH and third parties in furtherance of his wire fraud, false claims and identity theft schemes;

b. Information relating to the use of the criminal proceeds, the creation and maintenance of financial accounts, financial transfers and transactions, the possession of monetary instruments, the disbursement of funds;

c. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts;

d. Evidence indicating the email account holder's state of mind as it relates to the crime under investigation;

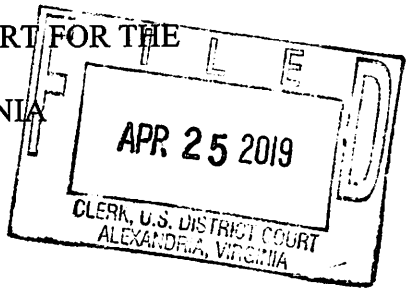
e. Information that would link the email account to other email accounts controlled by the subscriber;

f. Evidence indicating how and when the email account was accessed and used, including IP logs, passwords, geo-locational information or other records that will help establish the location of the account user;

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE EMAIL ACCCOUNT **HKULLAH@GMAIL.COM** THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE	Case No. 1:19-SW-445 **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT

I, Lisa Warffeli, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain email account, **hkullah@gmail.com** (herein referred to as the **"TARGET EMAIL ACCOUNT"**) that is stored at the premises controlled by Google, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The **TARGET EMAIL ACCOUNT** is assigned and used by Haroon K. Ullah ("ULLAH"), a government official, as described further below.

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government copies of the information, including the content of communications, further described in Attachment B. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement

officer is not required for the service or execution of this warrant. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a special agent with the U.S. Department of State ("DOS"), Office of Inspector General ("DOS OIG") and have been so employed since January 2017. Prior to employment with DOS OIG, I was a special agent for the U.S. Department of State's Bureau of Diplomatic Security for approximately ten years. Prior to becoming a special agent I practiced law in the Commonwealth of Virginia. In 2007, I completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia and the Bureau of Diplomatic Security's Basic Special Agent Course in Dunn Loring, Virginia. My current responsibilities include the investigation of violations of United States criminal laws, to include procurement fraud, grant fraud, false claims, bribery, conspiracy, kickbacks, money laundering, and other violations of laws affecting the programs and functions of the DOS and USAGM. During the course of my career, I have investigated or assisted in investigations concerning public corruption, white-collar crime, computer-related crimes, passport and visa fraud, sexual assault, and other complex investigations of fraud, waste, and abuse involving government funds. I hold a Bachelor's of Arts and Master of Arts degrees from George Mason University and a Juris Doctor degree from George Mason University School of Law.

4. The facts and information contained in this Affidavit are based upon my training and experience, personal knowledge, and observations during the course of this investigation, as well as the observations of other agents involved in this investigation. This Affidavit contains only the information necessary to support probable cause and is not intended to include each and every fact or matter observed by me or known to the government.

5. Based on the facts set forth in this Affidavit below as well as my training and experience, I submit that there is probable cause to believe that violations of 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 287 (False, Fictitious and Fraudulent Claims), and 18 U.S.C. § 1028A (Aggravated Identity Theft), have been committed by the user of the **TARGET EMAIL ACCOUNT**.

JURISDICTION AND VENUE

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

7. Although he also co-owned a condominium in the District of Columbia with his sister and worked in the District of Columbia, I believe that ULLAH resided in the Commonwealth and Eastern District of Virginia during the course of this scheme. ULLAH also maintained a bank account in the Eastern District of Virginia which received wire deposits of the reimbursements described below. Thus, I have reason to believe that ULLAH caused the transmission of interstate wires in and through the Eastern District of Virginia in furtherance or his scheme, involving banking, telephonic and other wire transactions.

STATEMENT OF PROBABLE CAUSE

Background

8. The U.S. Agency for Global Media ("USAGM") is a government agency based in Washington, D.C. USAGM was formerly known as the Broadcasting Board of Governors (BBG). USAGM is an independent federal agency that seeks to inform, engage, and connect people around the world in support of freedom and democracy. USAGM provides multimedia

broadcast distribution, as well as technical and administrative support to the broadcasting networks. It manages a global network of transmitting sites and an extensive system of leased satellite and fiber optic circuits, along with a rapidly growing Internet delivery system servicing all USAGM broadcasters. It is also the administrative and marketing arm of the Agency. USAGM also oversees five networks: two federal organizations — the Voice of America and the Office of Cuba Broadcasting, which oversees Radio and TV Marti — Radio Free Europe/Radio Liberty, Radio Free Asia and the Middle east Broadcasting Networks — which receive grants from USAGM.[1] USAGM, like BBG before it, is overseen by the Inspector General of the U.S. Department of State, for whom I work as a special agent.

9. ULLAH was the Chief Strategy Officer ("CSO") for USAGM and had been in that position since October 1, 2017, until he was placed on administrative leave and later terminated as discussed below. According to his on-line biography, ULLAH "leads the Agency's policy engagement within the broader U.S. government as well as with key stakeholders outside the federal government. The CSO focuses on strategic planning and initiatives to make the Agency more strategically relevant in the national security, foreign affairs, and global media spheres."[2] Before joining USAGM, ULLAH had been employed with the U.S. Department of State since 2010. ULLAH holds a Ph.D. degree, is a published author, and is a recognized expert in countering violent extremism.

10. In his capacity as CSO for USAGM, ULLAH was authorized to travel by USAGM at government expense only for official business. Such official travel for ULLAH's trips was arranged and authorized via E2 Solutions ("E2").

---

[1] *See* https://www.usagm.gov/who-we-are/organizational-chart/ (last visited January 24, 2019).

[2] *See* https://www.usagm.gov/who-we-are/management-team/ (last visited January 24, 2019).

11. ULLAH sought administrative assistance from USAGM staff to arrange his travel and to submit his vouchers into the E2 system for reimbursement by providing them with the receipts from his travel. Within E2, travelers are required to certify that the vouchers and documents they submit are true and accurate and that the traveler has not previously received payment for the expenses. Because ULLAH had administrative staff submit his vouchers within E2, the staff printed out the voucher along with the receipts and the certification form for ULLAH to sign in hard copy. ULLAH signed the certification form for each of his closed vouchers in E2.[3]

12. In or around September 2018, USAGM travel personnel questioned purported Sheraton and Marriott hotel invoices that ULLAH had submitted for reimbursement through E2 for official travel to Chicago and New York. USAGM travel personnel noted that the hotel invoices did not appear to be true Sheraton and Marriott invoices, due to the formatting and content. Moreover, the amount billed for the room in New York was suspicious because the typical taxes and fees in New York City appeared to be incorrectly calculated. USAGM personnel contacted the hotels and sent them copies of the suspicious invoices that ULLAH had submitted. Hotel personnel confirmed that ULLAH had not stayed at either hotel on the dates indicated; that the hotel invoices ULLAH had submitted did not match hotel-issued invoices; and that the hotel had not produced the invoices submitted by ULLAH.

13. I obtained these suspicious invoices from USAGM for further investigation. I have reviewed them. I requested from the hotels examples of true and correct invoices that they would have issued a traveler. I also obtained all the hotel invoices submitted by ULLAH to USAGM for reimbursement. I contacted these hotels as well to confirm the authenticity of the

[3] The certification contained the following language, "this voucher is true and correct to the best of my knowledge and belief, and that payment or credit has not been received by me."

invoices; whether ULLAH had stayed at their hotels; and to obtain examples of true and accurate invoices in the instances the invoices submitted by ULLAH were fabricated. My conclusion from my investigation is that ULLAH fabricated eleven (11) invoices he submitted to USAGM for reimbursement, as further discussed below.

14. On October 22, 2018, I interviewed ULLAH regarding his travel. ULLAH said his travel was "Just mostly work-related." When shown invoices for hotels submitted with his vouchers, ULLAH stated, "That's probably what I turned in." ULLAH also confirmed that handwriting, which appeared on some of the hotel invoices, was his handwriting.

15. Immediately after I interviewed ULLAH, USAGM placed ULLAH on paid administrative leave. When ULLAH was placed on leave, his official phones and computers were taken from him and he was walked out of the building. USAGM later terminated ULLAH on or about April 16, 2019.

16. On October 31, 2018, I submitted a preservation request to Google through its Law Enforcement Request System ("LERS").

17. On January 31, 2019, I submitted a renewal of the preservation request through LERS.

18. On February 11, 2019, a search warrant was issued for ULLAH's government email account by the U.S. District Court for the Eastern District of Virginia. Also, on February 13, 2019, the U.S. District Court for the District of Columbia issued a search warrant for ULLAH's office at USAGM headquarters and for ULLAH's work cell phone. All search warrants were executed on February 15, 2019.

Overview of Manner and Means of ULLAH's Scheme to Defraud

19. ULLAH devised a scheme to defraud USAGM of money and property by submitting for reimbursement falsified hotel invoices; falsified taxi receipts; double-billing sponsors and USAGM for the same trips; and billing USAGM for what appear to be personal trips, either to promote his book, or for week-end trips during which no USAGM business was likely conducted. Also, ULLAH submitted to USAGM a falsified and forged letter from a real medical doctor claiming that ULLAH required an upgrade to business class because of a medical condition. The doctor confirmed that the letter was a forgery; that he did not authorize ULLAH to use his identity; and that a business class upgrade for ULLAH's sore knee was not medically necessary. By stealing the doctor's identity, ULLAH, thus, also defrauded USAGM of all payments for business class upgrades, some of which were substantial, as they involved international flights. Altogether, based on a preliminary review of his travel records, it appears that ULLAH defrauded USAGM of at least $25,000, and committed aggravated identity theft in so doing.

20. Based upon my analysis of the falsified and fraudulent documents that ULLAH submitted to USAGM for reimbursement, it appears that he used various techniques to create hotel invoices. With some hotel invoices, ULLAH seems to have obtained logos of hotel chains and pasted them onto a document along with what appears to be Excel spreadsheets to create hotel invoices. With other hotel invoices, it appears he took a legitimate hotel invoice and changed his address or other data, possibly to conceal the hotel room had been paid by a third-party. It is possible he also obtained invoice creation software to create these invoices.

The Use of the TARGET EMAIL ACCOUNT

in Furtherance of the Scheme to Defraud

21. During the course of this investigation, I learned that ULLAH used the **TARGET EMAIL ACCOUNT** to schedule presentations and book signings for which he received compensation from organizations outside of USAGM while informing USAGM the purpose of his travel was for USAGM business.

22. I discovered the use of the **TARGET EMAIL ACCOUNT** when I was informed the address on a hotel invoice had been altered. ULLAH submitted an invoice from the Residence Inn in La Jolla, California as part of his voucher for trip 9566094. I provided a copy of the invoice submitted by ULLAH to an employee of the Residence Inn. The employee confirmed ULLAH stayed at the hotel on the dates indicated in the invoice, but upon further review noticed ULLAH's address was changed. The invoice submitted to USAGM by ULLAH listed his address as "330 Independen Wash DC," which is an abbreviation of USAGM's address of 330 Independence Avenue SW Washington, D.C. The Residence Inn employee stated that the address on the hotel's invoice was 112 West G St. #601 San Diego, California 92101, which was the mailing address for the World Affairs Council for San Diego (hereafter "WACSD'). A representative of the WACSD confirmed that the organization paid for ULLAH's stay at the Residence Inn and that the organization split ULLAH's other expenses with the World Affairs Council for Inland Southern California (hereafter "WACISC").

23. The WACISC provided me with copies of emails in which ULLAH used his USAGM email account to coordinate his presentations at both World Affairs Councils, to submit receipts for reimbursement, and to request that the WACISC reimburse ULLAH for his rental

car, since the organization was not charged for ULLAH's hotel room. ULLAH forwarded scheduling emails he exchanged with WACISC to the **TARGET EMAIL ACCOUNT**.

24. ULLAH stated in his authorization to USAGM that he needed to travel to Los Angeles and San Diego to meet with Fandago and "other analytic folks" as well as present at World Affairs Councils information on "Polygraph"[4] and "raise awareness on our very good of our storytellers." Both organizations confirmed that ULLAH was requested to speak about his book, not USAGM. The representative of the WACSD stated no one attending the presentation knew what USAGM was.

25. ULLAH also submitted to USAGM receipts for upgrades to business class per the medical release he submitted to USAGM as mentioned above. The upgrade receipts were emailed from United Airlines to the **TARGET EMAIL ACCOUNT**. The total for the upgrades was $1,343.00.

26. ULLAH provided USAGM with a letter allegedly written by a true medical doctor identified here as "the Doctor", on "The Bone and Joint Center" letterhead. The letter stated that ULLAH had a degenerative knee condition known as patella tendonopathy and for flights longer than one hour in duration he was to "lie flat."

27. On November 15, 2018, I interviewed the Doctor who stated he was not with The Bone and Joint Center and he had not written the letter that ULLAH submitted to USAGM. He said the signature on the false letter was not his and he would never require an accommodation of business class air travel for a patient. The Doctor knew ULLAH personally and had seen him once or twice as a patient. The Doctor confirmed that it was not medically necessary for ULLAH to travel in business class, and that he had never given ULLAH permission to sign his name or

[4] Polygraph refers to a data analytics company and not the lie detector test.

use his identity in furtherance of a reasonable accommodation or any claim for reimbursement from the government for travel expenses.

28. Based upon my conversations with the two World Affairs Councils, I then researched other World Affairs Councils in cities to which ULLAH traveled allegedly for USAGM business.

29. ULLAH submitted a travel voucher for E2 Trip 9018448 for travel to Boston from February 21 to February 23, 2018 for the purpose of meeting with "Digital Democracy" and "data teams" on USAGM. I learned from an Internet search that ULLAH gave a presentation at the World Affairs Council for Western Massachusetts (hereafter "WACWM") on February 21, 2018.[5] Records obtained from the WACWM contained email exchanges between WACWM and ULLAH using the **TARGET EMAIL ACCOUNT**. The email exchanges included ULLAH's publicist. The email exchanges did not discuss ULLAH discussing USAGM, but his new book and the sale of the book.

30. According to the WACWM, ULLAH's presentation was part of their "brown bag lunch" series. ULLAH's trip spanned three days. It is likely that the **TARGET EMAIL ACCOUNT** will contain communications with this and other organizations in an effort to promote his book.

31. ULLAH submitted a voucher to USAGM for E2 Trip 9361798 for travel to Boston on June 19, 2018. ULLAH stated the reason for the trip was "BBG Meetings. Through records obtained during the course of this investigation, I learned that ULLAH spoke at WorldBoston on June 19, 2018. From records provided by WorldBoston, I found that ULLAH

[5] "How Do We Stop the Next World War: The Weaponization of Information and the Fight for Cyber Supremacy,' *See* https://worldaffairscouncil.com/?page_id=231 (last visited January 24, 2019).

reached out to WorldBoston using the **TARGET EMAIL ACCOUNT** informing WorldBoston he had a new book and would like to give a presentation on the book at WorldBoston. WorldBoston invited ULLAH to speak on June 19, 2018 and sold copies of his book.

32. Through records obtained during the course of this investigation, I learned ULLAH spoke at WorldBoston on June 19, 2018. From records provided by WorldBoston, I found that ULLAH reached out to WorldBoston using the **TARGET EMAIL ACCOUNT** informing WorldBoston he had a new book and would like to give a presentation on the book at WorldBoston. WorldBoston invited ULLAH to speak on June 19 and sold copies of his book.

RELEVANCE OF THE TARGET EMAIL ACCOUNT

33. As indicated above, the documents I have obtained from third parties indicate that ULLAH used the **TARGET EMAIL ACCOUNT** to facilitate his appearances at speaking events during which his book was promoted and sold, but for which he billed USAGM as official travel. The **TARGET EMAIL ACCOUNT** was used for other travel-related purposes, and a search of the **TARGET EMAIL ACCOUNT** is likely to reveal the true purpose of the travel, or the absence of an official USAGM reason for travel. I also submit that there is probable cause to believe that the **TARGET EMAIL ACCOUNT** will contain invoices, receipts, and other evidence of ULLAH's travel. Likewise, it may contain templates, receipts, and communications showing the preparatory steps ULLAH took to create false documents, and otherwise will constitute evidence, fruits, and instrumentalities of the crimes described in this affidavit.

34. I know also from training and experience that individuals, including white collar criminals, tend to maintain such records for lengthy periods of time, especially when they are engaged in ongoing and uncharged criminal conduct. There are many reasons why criminal offenders maintain evidence for long periods of time. The evidence may be innocuous at first

glance (e.g., financial, credit card, travel documents, telephone directories, photographs), but have significance and relevance when considered in light of other evidence. The criminal offender may no longer realize he/she still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal offender may also be under the mistaken belief that he/she has deleted, hidden or further destroyed the evidence, which, in fact, may be retrievable by trained law enforcement personnel.

BACKGROUND CONCERNING EMAIL

35. From my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

36. A Google subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

37. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

38. From my training and experience, I know that email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e. session) times and durations, the types of services utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") from which a user accesses the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner.

39. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as

technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

40. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the

account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

41. In sum, based on the facts set forth in this Affidavit, I submit that there is probably cause to believe that the user of the **TARGET EMAIL ACCOUNT** did commit wire fraud, in violation of Title 18 U.S.C. §1343; aggravated identity theft, in violation of Title 18 U.S.C. §1028A; and submitted false claims, in violation of 18 U.S.C. § 287. Thus, I respectfully request the issuance of a Search Warrant for the **TARGET EMAIL ACCOUNT**. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully Submitted,

Lisa Warffeli
Special Agent, United States Department of State,
Office of the Inspector General

Subscribed and sworn to before me
this 23 day of April, 2019.

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

The Honorable Theresa Carroll Buchanan
United States Magistrate Judge

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the following email account:

hkullah@gmail.com

which is stored at premises controlled by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google

For the account listed in Attachment A, to the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any e-mails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved since October 31, 2018, Google is required to disclose the following information to the government for the period of account inception to the present:

a. The contents of all electronic communications associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, files, all attachments to emails and other communications (including the native files), the source and destination addresses associated with each communication, all email header information, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All device information associated with the account;

e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, chat lists, calendar data, pictures, and files;

f. All records pertaining to communications between USAGM and any person regarding the account, including contacts with support services and records of actions taken.

g. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of wire fraud (18 U.S.C. § 1343), aggravated identity theft (18 U.S.C. § 1028A), and false claims (18 U.S.C. § 287), involving HAROON K. ULLAH and any other co-conspirators, including, for the email account listed on Attachment A, information pertaining to the following matters:

a. The email and information will contain evidence that ULLAH is involved in defrauding the United States through the submission of fraudulent vouchers and falsified supporting invoices and receipts, as described in the Affidavit in support of probable cause. The account will contain evidence of communications between ULLAH and third parties in furtherance of his wire fraud, false claims and identity theft schemes;

b. Information relating to the use of the criminal proceeds, the creation and maintenance of financial accounts, financial transfers and transactions, the possession of monetary instruments, the disbursement of funds;

c. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts;

d. Evidence indicating the email account holder's state of mind as it relates to the crime under investigation;

e. Information that would link the email account to other email accounts controlled by the subscriber;

f. Evidence indicating how and when the email account was accessed and used, including IP logs, passwords, geo-locational information or other records that will help establish the location of the account user;

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, and my official title is _____. I am a custodian of records for Google. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google; and

c. such records were made by Google as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature